Security and QoS Integration for Protecting Service Providers in Heterogeneous Environments

Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae

Abstract—**Similar to the Internet, connectivity in Next Generation Networks such as 4G will be IP-Based. This implies that they inherit all the security problems of the current Internet. Amongst these numerous threats, compromise and resource exhaustion threats which come in the form of Denial of Service attacks, are very common and particularly serious. The severity of such attacks will be fuelled by the development of heterogeneous devices which have several wireless interfaces, as multi-homed devices will be able to send multiple connection requests to the server and thus launch attacks over different access networks. This paper details a new model to address the problem of Denial of Service attacks against the current Internet which limit the accessibility of a server based on its operational scope such that the solution will work effectively in heterogeneous, multi-homed environments. However, Denial of service attacks target the system resources and degrade their performance thus, affecting the Quality of Service's delivery to the subscribed users. Therefore, the proposed model suggests dealing with security and QoS in an integrated manner by using the concept of Quality of Security Service where security is considered as a Quality of Service' parameter. This paper furthermore shows how security can be integrated into the infrastructure of future network systems. However, in order to implement the proposed model, it is necessary to enhance current networking infrastructure by extending current services such as the Domain Naming Service and evolving new services such as a Master Locator to support user mobility.**

Index Terms—**Heterogeneous Environment, The Scope Concept, Multi-Homed Devices, Denial Of Service Attack, Distributed Denial Of Service Attack.**

I. Introduction

SECURITY and Quality of Service (QoS) are two crucial issues for safe and adequate network operation. Although they affect the entire network infrastructure, in many operational scenarios, QoS and security are managed by different groups, the implementation of them will have an impact on each other. Without information about the available security level and the desired requirements, a poor assignment of the QoS parameters may lead to denial of service for vital but low bandwidth data. In contrast, an ignorance of the QoS requirements with the implementation of high security level may reduce the effectiveness of the offered QoS.

The authors believe that, by integrating network QoS and security, issues such as the secure delivery of QoS parameters during connection setup, data protection during transmission as well as immunity against denial of service attacks can be achieved. If security mechanisms such as authentication, authorization and access control are enforced during the QoS signalling stage, this will help in providing secure access and authorized resource reservation. Additionally, considering the QoS requirement while determining the security parameters such as the encryption algorithms and the length of the keys will provide secure transmission path as well as content protection without any contradictions with the QoS performance.

Therefore, QoS and security must be considered together in the design of any future communication framework. This integration is of most significance in Next Generation Networks (NGNs), where the core network is not owned by a sole operator. This is due to the fact that in this environment, multiple network operators each with different QoS and security measurement must collaborate in an open architecture, and thus providing an End-to-End QoS as well as cross-operators security will be the among the factors that needs to be addressed in the heterogeneous networks. Therefore, in future networks, there is a need for new mechanisms that would enable the integration and identify conflicts in security and QoS requirements. However, for such mechanisms to work efficiently in the future heterogeneous environments, they need to get sufficient information about the different network systems as well as security and QoS requirements. This situation highlights the need for re-examining the network infrastructure and proposing new functionalities to support the QoS and Security integration.

This paper introduces an integrated model of QoS and security to protect end servers in heterogeneous environments. The model benefits from recently introduced enhancements on the network infrastructure [8] [14] to limit servers accessibility to their operational scopes. By integrating QoS and security in the proposed model, only legitimate nodes within the servers' defined scope could contact them. Furthermore, the model will monitor the utilization of the network resources by the corresponding nodes to make sure that they cannot exceed their agreed QoS, and thus, the model succeeded in stopping Denial of Service (DoS) attacks while mitigating the distributed ones (DDOS).

The rest of this paper is organized as follows: Section 2 defines the problem of denial of service attacks in heterogeneous environments. Section 3 describes the QoS and security integration through the concept of QoSS. Section 4 investigates the issue of providing QoS in heterogeneous networks by viewing the structure of future networks along with the operation entities, and then explaining a potential framework for signalling QoS in different scenarios such as connection initiation and handover. While Section 5 analyses different approaches in the literature to hide the identity of servers. Section 6 describes the work to limit servers accessibility in heterogeneous environments; it starts by explaining recent work, which dealt with the multi-homing issue and defined scope concept to restrict the reachability of servers in heterogeneous environments. The sections also, introduces and analyses the proposed security model to restrict servers accessibility based on their operational scope while considering the utilization of the network resource. The

M. Aiash is with the Department of Engineering and Information Systems (EIS), Middlesex University, London, UK e-mail: M.Aiash@mdx.ac.uk.
G. Mapp and A. Lasebae are Senior Lecturers at Middlesex University.

paper concludes in Section 7.

II. Problem Definition

Future communication systems must allow ubiquitous connectivity where users are always connected from anywhere and at any time. The need for continuous connection is being met by the development and deployment of a number of wireless technologies including 3G/HSPDA, WLAN [15] with Long Term Evolution (LTE) [23] and Wimax being the latest network of being deployed. However with the wide-scale deployment of wireless networks as end-systems, there will now be significant differences in network characteristics in terms of bandwidth, latency, packet loss and error characteristics. These developments imply that the future Internet will not have a single unified infrastructure rather it will comprise a fast core network with slower peripheral networks attached around the core. The core network will consist of a super-fast backbone using optical switches and fast access networks which use Multiple Protocol Label Switching (MPLS). Most of the peripheral networks will be based on wireless technologies. In this environment, future mobile terminals will be connected using several network interface cards (NICs), which enable them to switch between any of the supported networks while remaining connected to end servers. This is referred to as seamless Vertical Handover (VH), which has been under investigation by many research effort such as the IEEE 802.21 [22] and the Y-Comm group [7].

This open and multi-homed nature of the Next Generation Networks (NGNs), make them vulnerable to QoS and security threats. On one hand, in this heterogeneous environment, there is a need for an end-to-end, cross-operators QoS provision. When users subscribe to a specific service, this implies that the two end systems have to agree on certain conditions of using the service, this is known as the Service-Level of Agreement (SLA). The SLA includes contracted delivery time (of the service) along with its performance. In the case of a single operator scenario, where all the resources are controlled and managed by one administrative entity, maintaining the SLA would not be an issue. However, this will not be the case in multiple operators environment, where the mobile terminal roams among access networks, controlled by different operators. In this open architecture each operator has control only over the resources in its own domain and not the resources of the other domains. Therefore, when a mobile terminal moves into another domain, the old operator cannot any more guarantee the agreed on QoS.

To address these threats, different research efforts have been trying to deal with the QoS issue by proposing frameworks for End-To-End QoS signalling such as the Daidalos II and the Y-Comm QoS frameworks [16] [8].

On the other hand, the open and multi-homed nature of the Next Generation Networks (NGNs), makes them vulnerable to security threats such as the compromise and resource exhaustion attacks. While the first takes the victim offline, the latter leaves the server intact but however overloads it with a huge volume of traffic and thus preventing it from serving legitimate clients. These two attacks target service availability and thus, are categorized as forms of Denial of Service (DoS) attacks. Due to many factors, these attacks will become more common in future, heterogeneous networks: firstly, the concept of global reachability, which has been adopted in the design of most communication protocols, allows any host to communicate with any other hosts over the globe. Secondly, due to the absence of QoS-provision over the different networks, an attacker can send a huge volume of traffic towards the victim without any indication of a QoS-breach. Thirdly, multi-homing issues in future networks will increase the severity of these attacks in heterogeneous environments, as malicious, multi-homed devices use several interfaces, identified by different network addresses to launch the attack, without having anything to indicate that these addresses are collocated on the same node.

It is obvious that, the compromise and resource exhaustion attacks lead to a breach of the agreed SLA. This highlights the need for an integrated solution that considers the security and QoS sides of these attacks. Moreover, in order to deal with the above situation, there is a need for a novel approach that addresses each of the afore-mentioned factors. Therefore, to deal with the first factor, the proposed approach in this paper enhances the concept of the " Off By Default" [3] , which enables the end-hosts or servers to define the nodes to communicate with and thus, limits servers accessibility based on their preference. Secondly, in order to deal with the QoS side of this problem, there is a need to monitor the utilization of the resources, allocated for the connection over the different networks and make sure that there is no breach of the agreed QoS. Therefore, the proposed approach adopts the structure of heterogeneous networks and the end-to-end QoS framework, presented in [8]. This structure defines dedicated network entities to monitor the network's utilization and make sure that the Corresponding Node (CN) cannot exceed the agreed QoS. The third factor is the issue of multi-homing, which has been investigated by different research efforts such [9][10][11] [12]. To deal with the multi-homing issue, new naming service and locating systems, namely the Enhanced Domain Name System (eDNS) and the Master Locator (ML) were introduced in [14].

III. QoS and Security Integration

QoS and security are two crucial issues in today's internetworking. While security provides proof of identity, preserves data integrity and confidentiality as well as supports authorized access to the resources, QoS refers to the ability of providing different priority to different application and users to guarantee a certain level of the performance to a data flow. In this sense, QoS mechanisms refer to resource reservation control mechanisms as well as the performance of the services.

Security and QoS are not quite independent, since the choice of security mechanisms may affect the delivery of the QoS and visa versa. Security mechanisms ensure appropriate service assignment and billing; a selection of poor security mechanisms might expose the system and make it vulnerable to security threats such as Denial of Service Attack (DoS) which, will reduce the performance of the network or end servers, while inappropriate QoS selection might be in conflict with the security level and lead to a security breach. For instance, providing a very high performance for some time-sensitive service, might require reducing the level of the service security. This interaction implies that, both QoS and security must be considered together when designing

and implementing a network infrastructure to achieve the best possible security and QoS level. In order to support this integration between QoS and security, the concept of Quality of Security Service (QoSS) has been investigated by different research efforts such as [25] [26] [27]. The QoSS represents adaptive security enforcement mechanisms that support dynamic security policies and services, it can be applied to computing and communication systems at all levels of technology, from applications to base protocols and architectures and encompasses many aspects of security research, including Quality of Protection, Adaptive Security, Dynamic Security, Policy-Based Access Control. In this concept security has been managed as a dimension of Quality of Service with the aim of leveraging existing security mechanisms to improve availability, predictability, and efficiency, while maintaining, if not increasing the overall security.

However, such integration between the QoS and security within the concept of QoSS has to be carefully considered. Since QoS involves users requesting for variable levels of services, that are related to the performance of the underlying systems, for security to be a real part of QoS, security choices must be presented to users, and the QoS mechanism must be able to modulate related variables to provide predictable security service levels to those users. By introducing variable level of security parameters, for example, different encryption and authentication mechanisms and variable length of keys, results in additional parameters, the QoS mechanism has to consider as well as solve any conflict in order to meet overall user and system demands, as well as balance costs and projected benefits to specific users/clients. Nevertheless, considering the various levels of security as a dimension of the QoS mechanism means that it can adapt more gracefully to dynamic changes in resource availability, and thereby do a better job at maintaining requested or required levels of service in all of its dimensions, which is in essence is the premise of QoSS.

IV. Providing QoS in Heterogeneous Environments

This section describes our work, which has recently been presented in [8], to propose a QoS framework in heterogeneous environments. The section starts by briefly viewing a potential structure of future networks along with its operational entities, it then explains the three targeted QoS-Signalling models, which are responsible for providing QoS in different scenarios.

A. Overview of Future Networks

Unlike the closed environments in current mobile systems (2/3G), the core network in future systems will not be controlled by a sole operator [17], rather multiple operators will coexist in the core network and provide clients with ubiquitous connectivity. However, since each network operator uses a different network architecture, interoperability is the major challenging problem.

One proposed solution to this problem is having a central management entity to control the resource of the all different technologies and coordinate the multiple operators.

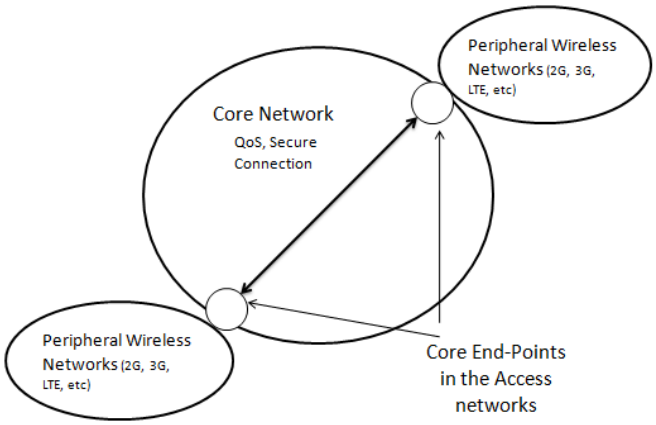

Fig. 1. Future Internet Structure

The concept of a central management entity was recommended by the ITU-T recommendation for NGN as in [21]. The recommendation proposes the concept of Regulatory Authority which controls different network operators and service providers. The Regulatory Authorities are regulatory bodies with the power to influence policies in telecommunication services, they are responsible for creating national policies to encourage the development of telecommunications, also they provide essential powers to regulate license agreements, interconnection arrangements, and monitoring unlawful telecommunication activities.

This concept of a central management entity in the local area was adopted and enhanced by the Y-Comm group [20] and Daidalos II [16] which introduced the concept of the Core End-Point (CEP) in [8] as an administrative domain for multiple, technology-specific networks. As shown in Fig 1, the future Internet could be viewed as composed of several Core End-Points, interconnected over the super fast backbone of the Internet. Each CEP is responsible for managing multiple, wireless peripheral networks such as Wimax, WiFi or cellular technologies.

A detailed view of the network along with its components are explained in the [8] and shown in Fig 2. It is a hierarchical structure of the network composed of three levels. The top level is the Core End-Point (CEP) which acts as a gateway to the Internet and is responsible for managing multiple, mid-level domains. Each domain is technology-specific and is controlled by a single operator. For instance the CEP might be connected to two domains, each is controlled by different technology operator such as WiMAX and GSM. The bottom level is the peripheral wireless networks, represented by multiple Access Routers (ARs), which make the interface between the network and the mobile terminal (MT).

Although the structure in Fig 2 is for future networks, it was evolved from the architecture of current systems; for instance, the technologies-specific domains in the mid-level correspond to the circuit switching and packet switching core networks in the GSM and GPRS or UMTS. The major difference is that the proposed structure proposes an open architecture, where different technologies and operators could join the network. However, to control this open architecture, the Core End-Point in the top-level must manage the resources in all various domains.

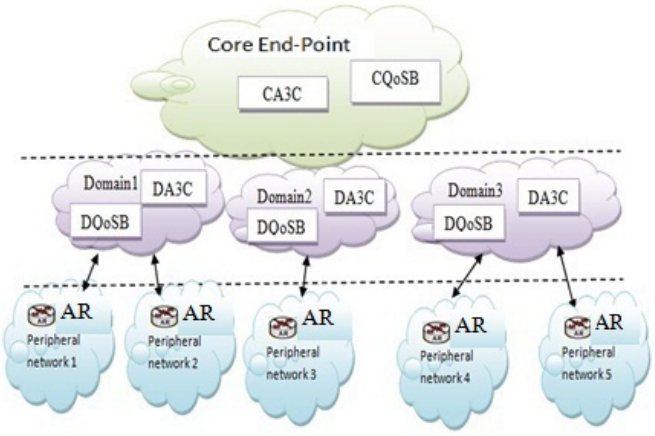

Fig. 2. Detailed network Structure

B. Supporting an End-To-End QoS in Heterogeneous Networks

As shown in Fig 2, in order to deal with the QoS and security tasks in this architecture, a number of operational entities have been proposed as follows:

- **The Central A3C server (CA3C):** This is the central Authentication, Authorization; Accounting and Cost (A3C) server in the Core End-Point. The CA3C holds the Service Level of Agreements (SLAs) along with the Network Level of Agreements (NLAs), which describe the clients' term of use of the service and access networks, respectively.
- **The Central QoS Broker (CQoSB):** is responsible for negotiating QoS in case of cross-CEP handover.
- **The Domain A3C Server (DA3C):** The DA3C is responsible for handling users' service aspects. Initially, it extracts user profile information from the CA3C and uses this information for authorizing the users' requests to access services..
- **The Domain QoS Broker (DQoSB):** manages the resources of the attached peripheral networks with respect user preferences and network availability, it also makes a per-flow admission control decision.
- **The Access Router (AR):** This is the link between the domain and the peripheral networks; it enforces the admission control decision, taken by the DQoSB. Since the AR acts as a relay between the Mobile Terminal (MT) in the peripheral network and the DA3C, using security terminology, the AR will be referred to as the Authenticator (Auth).

Although, a detailed explanation of the structure of these components has been introduced in [8], for the sake of this paper and in order to explain the proposed security model we need to briefly recall the structure of the CQoSB, DQoSBs and the Access Routers (ARs), which are among the key entities for the operation of the proposed security model.

As shown in Fig 3, the CQoSB comprises three modules: the QoSB Engine manages inter-domain connection and provides end-to-end QoS across administrative domains, the A3C interface is used for the interaction with the CA3C server. The High-level Access Admission (HAAD) module makes a per connection access control policy which will be passed to other operational entities in the network such as

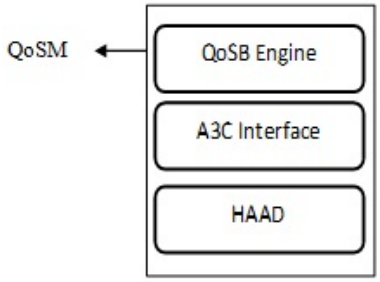

Fig. 3. The Central QoS Broker Structure

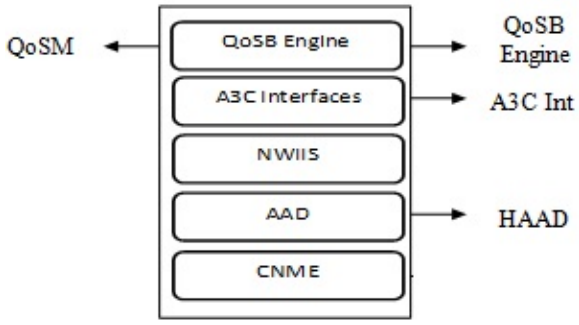

Fig. 4. The Domain QoS Broker Structure

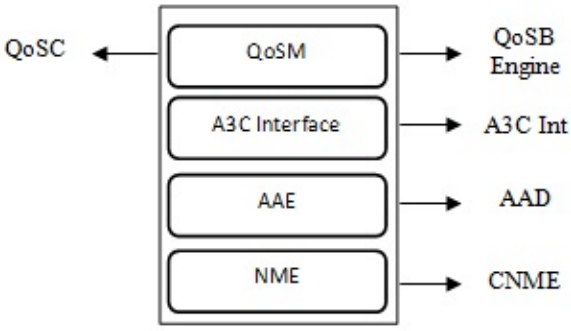

Fig. 5. The Access Router Structure

the DQoSBs and the ARs.

Fig 4 presents the structure of the DQoSB which comprises five interfaces. However, in this section we are only concerned about the Access Admission Decision (AAD) module; details about the other interfaces are found in [8]. The AAD acts as a proxy for the HAAD, and provides the AAE in the AR with policy- related decisions.

As shown in Fig 5, the AR comprises four interfaces: the QoS Manager (QoSM), the A3C interface; the Access Admission Enforcement (AAE) which enforces the access decision taken by the HAAD and the Network Monitoring Entity (NME)

For the connection between the AAE and AAD, there is a need for a policy information and configuration exchange protocol such Common Open Policy Service (COPS) [18], where the AR acts as an AAE and the an AAD.

These entities cooperate to provide security and QoS-related tasks. However, since there is a need for QoS provision in different situations, three QoS-Signalling models have been proposed in [8]:

- **The Registration Model:** describes the procedure followed when the MT first attaches to the peripheral

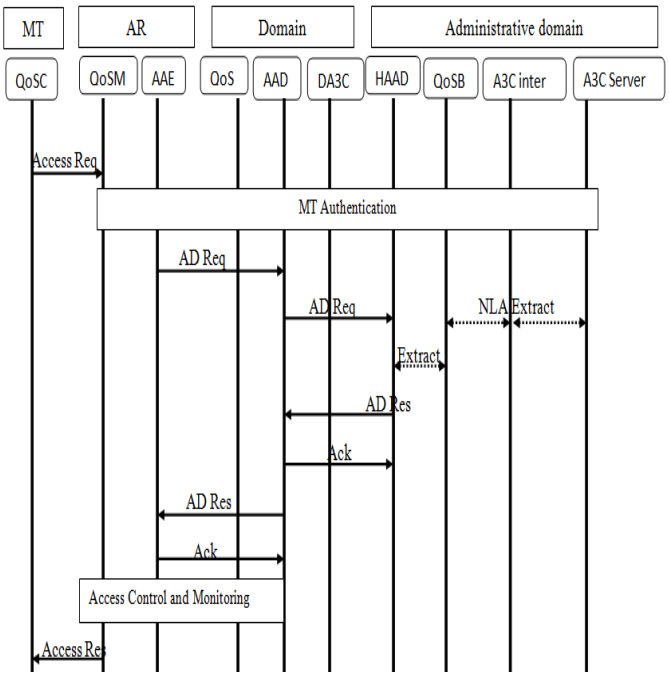

Fig. 6. The Initial Registration Model

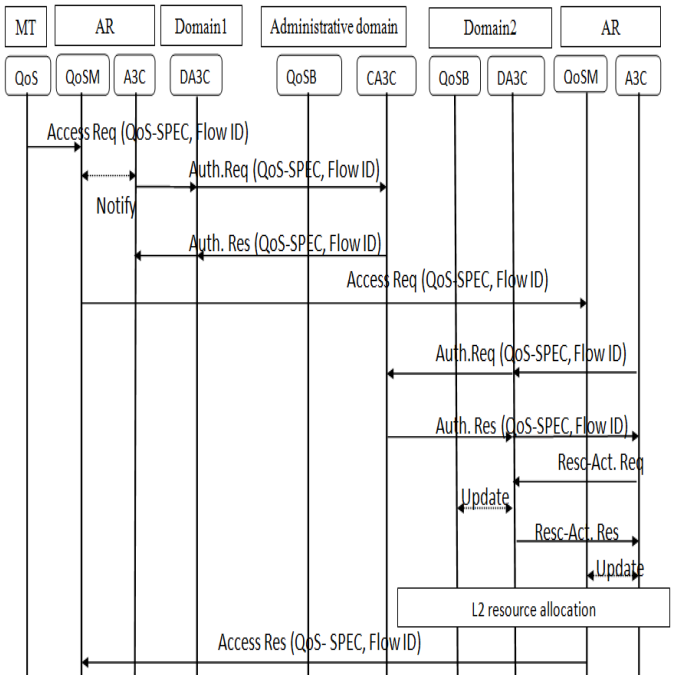

Fig. 7. The Connection Initiation Model

network. This model basically involves Authenticating the MT to use the network, then enforcing the access control policies based on the MT's SLA.

Initially, upon subscribing to the service, the user and the Central QoS Broker (CQoSB) share the details of SLAs which include the subscribed services and the type of the access network along with corresponding range of the desired security and QoS. As shown in Fig 6, once the mobile terminal is authenticated to access the network, the Access Admission Enforcement (AAE) module in the Access Router requests a user-specific Access Decision (AD Req) from the Access Admission Decision (AAD) module in the Domain QoS Broker. Since, this is an initial registration model, the AAD approaches the High level AAD (HAAD), which extract the user's profile from the QoSB Engine and passes the decision - via (AD Res) message- all the way back to the AAE module of the Access Router. The access policy is configured on the access router and an acknowledgement is sent back to the AAD.

- **The Connection Initiation Model:** deals with the case when the MT starts a connection to a server SP. It involves authorizing the connection request in both the source and the destination networks and making sure that it complies with the pre-agreed on QoS.

  As shown in Fig 7 shows a scenario of a mobile terminal MT willing to communicate with a server (S), where they are both residing in the same Core End-Point (Administrative Domain) but in different domains. The procedure starts when the MT expresses its intention by sending an Access Request with the desired QoS. However, before the MT could use the network, its request has to be authorized; therefore, using the A3C interface, the Access Router issues an Authorization Request (Auth.Req) with the QoS, required by the MT. The Central QoS broker and the A3C in the Core End Point will check the parameters in Auth.Req and based on the MT's SLA and the capabilities of the network, the request might be rejected or accepted. In case of acceptance, similar check has to be carried out for the destination network (the server's network). Once this is achieved, layer 2 resources in both networks are prepared to accommodate the connection.
- **The Handover Model:** This step explains the QoS provision in the case of Inter and Intra administrative domain handover. Fig 8 shows the case of Intra-Core End-Point handover, where the MT moves between different domains within the same Core End-Point(Administrative Domain), this model deploys the Pre-Authentication (Pre-AKA) protocol to achieve Pre-Authentication and Key Agreement as well as launching the security materials in the target network before the actual handover takes place and thus, reduce the disturbance to the handover caused by the security mechanisms. Also in this step, the QoS-context is transferred and used by the access control mechanism in the new network to enforce the right access admission policy. After configuring the access policy in the target Access Router, it starts L2 resources reservation and a successful handover response message is sent back to MT to trigger the actual handover.

  In the case of an Inter-Core End-Point handover, the user's SLA details are moved to the new Core End-Point; thus, the MTs related information becomes available in the target network. Then similar to the Intra-Handover scenario, access admission policy is configured and enforced by the AR and an acknowledgement is sent back to the MT to start the actual handover.

More details about these models are found in [8].

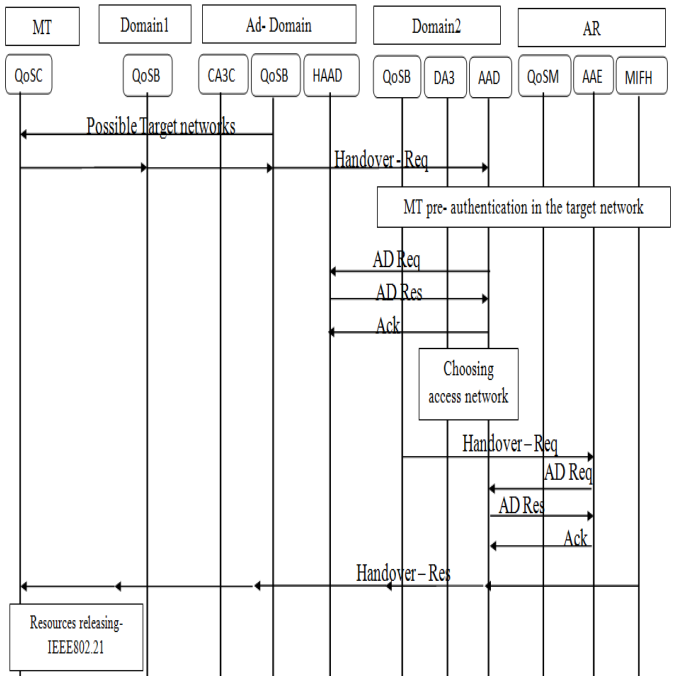

Fig. 8. The Intra-Handover Model

V. Limiting Servers Accessibility Over the Internet

One obvious solution to deal with the compromise and resource exhaustion attacks, which compromise the security and reduce the performance of the systems, is by controlling access to the victim. The literature is rich with mechanisms that have attempted to hide the server's identity and limit its accessibility, some of which are as follows:

A. Access Control Lists and Firewalls

One of the earliest attempts to enforce access control was by configuring ACLs on the network's routers, ACLs provide basic packet filtering to protect the networks from the outside world [5]; they filter the traffic and based on pre-configured criteria such as the Source/destination IP address or ports numbers, they will forward or block packets on the interface routers. As stated in [5], configuring ACLs on the edge routers could mitigate many threats such as IP spoofing and DoS TCP SYN flooding. However, configuring ACLs is an error-prone procedure and for each traffic type a new rule has to be added. Additionally, ACLs perform stateless packet inspection without considering the state of the whole session.

Firewalls address the shortages of basic ACLs, provide layered defence mechanisms; perform stateful packet inspection and have application awareness for a few transport protocols. This offers a higher level of protection than basic packet filtering. The firewalls also consider the state of the connection and thus, differentiate between packets belonging to different sessions. However, the problem with the firewall is that, it breaks a single session into two connections which, can have detrimental effects on end-to-end performance.

B. Network Address Translation

The idea of hiding the identity of the servers from external entities was initially proposed by the Network Address Translation (NAT) [1] where the NAT server acts as an IP converter that maps private IP addresses (the ones used in the internal network) to globally, registered addresses, in an attempt to allow hosts in private networks to transparently communicate with external hosts and visa versa.

However, the implementation of the NAT does not come without potential drawbacks. For instance, the connection between the hosts residing behind the NAT is broken on the first NAT-supporting router; this contradicts with the end-to-end concept which used to be the core principle of the current Internet [4]. Additionally, there are serious concerns about the operability of the NAT and Firewalls as well as the scalability of the NAT database.

TABLE I
A Brief Description of the Related Approaches

The Mechanism	Advantages	Disadvantages
ACLs	Mitigates IP spoofing and DoS TCP SYN flooding	Provides only stateless packet inspection.
Firewalls	Support layered defence mechanism and stateful packet filtering	Break the end-to-end connection's property, adds-on security mechanism that is vulnerable to configuration error
NAT	Less administrative effort, was the first to hide the identity of the server rather than preventing packets from getting to it	Contradicts with the end-to-end concept, interoperability problems with the Firewalls and newer version of IP addresses.
Off By Default	More integrated than the previous mechanisms	Place a burden on the network infrastructure, Not fully integrated.

C. Off By Default

To reduce the complexity and the overhead resulting from implementing the previous mechanisms, the authors in [3] proposed an integrated, access control-based approach through which, the host explicitly specifies the traffic it wants routed to it; thus defining its reachability. In this approach, the routers will not automatically route the packets unless explicitly directed to do so by the destination host.

This proposal however suffers from a number of drawbacks: Firstly, this approach requires the network to maintain accessibility information for each destination, this might place a burden on the network infrastructure. Secondly, the end host should be able to regulate its reachability for a wide spectrum of applications and protocols, update it in case of any modification, and then convey this information to the access router in a systematic way. Table I summarizes the pros and cons of the access control mechanisms.

Although, the approach of "Off By Default" has addressed many drawbacks of the primitive access control mechanisms, for this approach to be deployed in future heterogeneous networks, it requires major modifications and enhancements such as:

1) Currently, with the "Off By Default", the server could choose the hosts it wants to accept traffic from, this approach is not scalable. To deal with this situation, it

might be better for the server to set more general rules to determine its accessibility rather than specifying access rules per host.

2) Although, the "Off By Default" provided a certain degree of integration, the server still needs to explicitly specify its reachability to the gateway router which will propagate this to all routers via routing table update procedure. We agree that the gateway router must be aware of the server's accessibility, however, the process of conveying this information outside the network should be accomplished with a minimum involvement of the server. Additionally, we believe that only concerned entities should know the server's accessibility.
3) Considering the multi-homed nature of future devices, where a multi-homed device might choose to access the server over a different interface and using a new IP address, which is not known for the server. In such cases, the device will be banned from accessing the server although, it is eligible for it. Or in contrast, a multi-homed device might succeed in connecting to the server using different network interfaces with different IP addresses, and reserves more resource than it requires.
4) After making the connection, there is a need for monitoring the utilization of the network resources and making sure that there will not be a violation of the agreed SLA.

These points highlight the need for a new approach that could work effectively in the multi-homed, heterogeneous environments.

VI. Limiting Servers Accessibility in Heterogeneous Environment Using the Scope Concept

This section presents our proposed security model to limit the reachability servers in heterogeneous environments such as the one shown in Fig 2. Although the proposed model is based on the " Off By Default" concept, it has avoided most of its drawbacks such as being fully integrated with the network infrastructure. It also introduced new enhancements by considering the multi-homing and QoS issues.

However, the proposed mode benefited from some recent research of our group, which has been trying to address issues such as the multi-homing.

A. Investigating the Multi-Homing issue in Future Networks

In recent work of the Y-Comm group [13][14], the impact of multi-homed devices on current network addresses and structure has been investigated. The outcome highlighted the need for a new approach to map multiple network interfaces to the hosting device, thus a novel addressing scheme has been introduced in[13]. Additionally, major changes to location and naming systems such as the Home Location Register (HLR) and the Domain Name System (DNS) [19][6] have been introduced in [14].

Fig 9 shows the novel addressing scheme, the 128-bit long address has three portions: the Location_ID defines the domain of the mobile node (MN), the Node_ID is a 64-bit used to identify the node and is assigned by the manufacturer. Among the fields of the NetAdmin part is the 2-bit Scope Field (SF) which is responsible for defining the node accessibility as follow:

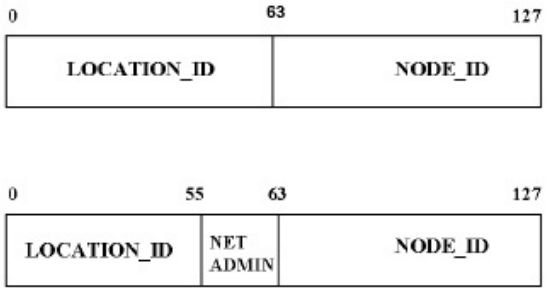

Fig. 9. The New Addressing Scheme

TABLE II
The eDNS Record

Internet Name	Node_ID	S	M	SF	Location_ID	ML's Address
Name1	Node_ID1	1	0	01	Location_ID1	ML- Add
Name2	Node_ID2	1	0	10	Location_ID2.1 Location_ID2.2	ML- Add
Name3	Node_ID3	0	0	11	Location_ID3	ML- Add
Name4	Node_ID4	0	0	10	Location_ID4.1 Location_ID4.2 Location_ID4.3 Location_ID4.4	ML- Add

- SF=00: indicates that the node could only be accessed by processes on the same machine.
- SF=01: defines a LAN scope which means that the node could be accessed from only the devices belonging to its LAN network.
- SF=10: denotes that only devices residing in the same site as the node could get access.
- SF=11: means that the device is globally accessible.

To support the new addresses and deals with the multi-homing issue, there is a need for major changes to the DNS and the location systems. Therefore, in [14] the group has proposed the concept of the Enhanced DNS (eDNS) and the Master Locator (ML), respectively. Similarly to the current DNS, the eDNS is still responsible for resolving Addresses to names and visa-versa. However, as shown in Table II, to support the new addressing scheme, there is a need to have more information about the node launched in the naming system. Examples of this information is the scope field (SF), the M and S fields, which are taken from the NetField portion of the address and indicate whether the destination is static and represent a multicast address. The ML is an evolved version of the Home Location Register HLR and is responsible for tracking the mobile terminal over different networks, Table III shows the structure of the ML.

B. The Proposed Security Model

In order to address the shortages of "Off By Default" and to provide a systematic approach to define and enforce servers' reachability, we introduce the scope concept, which limits servers' visibility over the network based on their functionality. The approach benefits from the new addressing

TABLE III
THE MASTER LOCATOR RECORD

Node_ID	Location_ID	INF	Mobility Vector	QoS Specifications
Node_ID1	Location_ID1.1 Location_ID1.2	INF1.1 INF1.2	Value1 Value2	QoS-Spec1 QoS-Spec2
Node_ID2	Location_ID2.1 Location_ID2.2	INF2.1 INF2.2	Value3 Value4	QoS-Spec3 QoS-Spec4

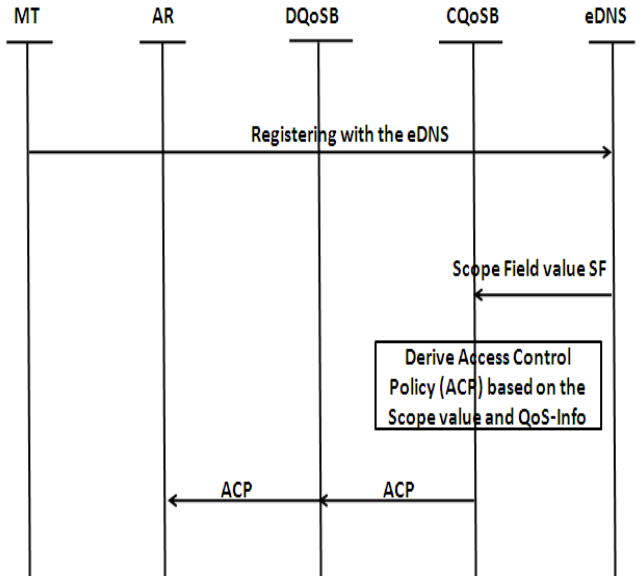

Fig. 10. Enforcing the Reachability Based on the Scope

scheme in section VI-A and uses the SF field to define the server scope.

However, for the proposed security model to work in future, heterogeneous environment such as the one in section IV-A, the SF field in the new address must be redefined and mapped to the network structure in Fig 2. In this structure of the network, a server could be local, accessed by client in the same peripheral network or by clients residing within the Core-End Point (CEP). The server might also be global and thus, accessible globally over the Internet. By considering the value of the (SF) field in the addressing scheme, the four scopes could be redefined as follows:

- SF=00: indicates that the node could only access locally via mechanism such as the loopback interfaces.
- SF=01: defines a LAN scope which means that the host could be accessed by the nodes in the same peripheral network. So the location _ID should be the local LAN.
- SF=10: denotes that the host could only be accessed by devices residing within the same Core End-Point. So Location_ID must be a site Address.
- SF=11: means that the device is globally accessible over the Internet.

The following sections explain how the servers' accessibility could be implemented and enforced using the new addressing scheme and the hierarchical network structure.

1) The host registration and devising the Access Policy : As shown Fig 10, in this stage, the hosts register themselves in a global naming system such as the proposed eDNS along with the corresponding Scope Field's value that reflects their scope, this information is passed to the High-level Access Admission (HAAD) module in the Central QoS Broker

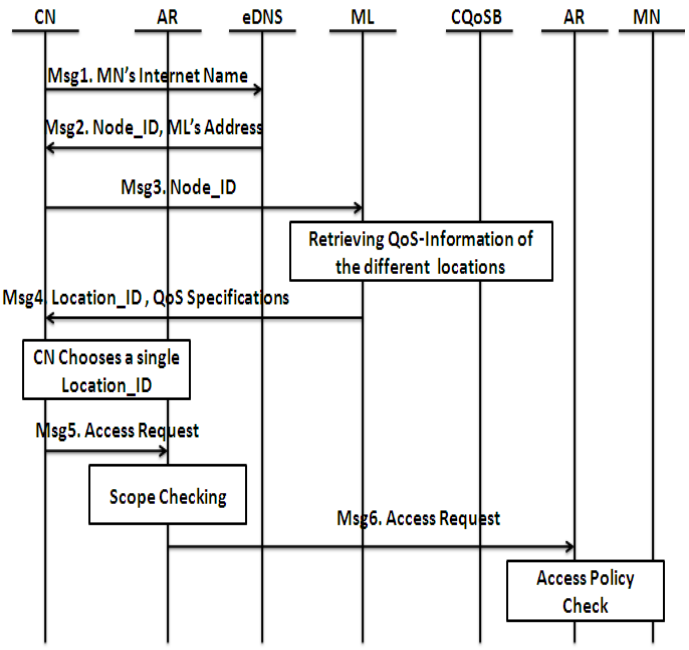

Fig. 11. Enforcing the Reachability Based on the Scope

(CQoSB). The HAAD uses the defined scope along with the Service Level of Agreement (SLA) information, retrieved from the QoS Engine to devise an Access Control Policy (ACP). The ACP is passed from the HAAD all the way to the Access Admission Enforcement (AAE) module in the Access Router (AR) using policy-conveying protocols such as the COPS protocol.

2) Enforcing the Access Policy: At the end of the previous stage, the end-hosts should have been registered with the eDNS along with their desired accessibility. Additionally, based on the accessible scope and other QoS-related information, an access policy will be devised by the HAAD and transferred to the enforcement module in the AR which will, based on the policy, accept or drop access requests.

Fig 11 shows the transaction in the case of the Corresponding Node (CN) trying to connect to a mobile node (MN). For this scenario, we presume that, MN's scope might be any of the LAN, Domain or Global.

- **Msg1**: The CN asks the eDNS sever for MN's address.
- **Msg2**: The eDNS uses the MN's name to look up its database and since the MN is a multi-homed device, its name will be resolved to different addresses with the same Node_ID, this implies that the MN is accessible over different routes/ networks. However, the eDNS cannot define the best route for the connection. Therefore, the eDNS returns the MN's Node_ID and the address of the Master Locator(ML) that manages the mobility of MN.
- **Msg3**: The CN polls the ML to find out the different networks to which the MN is currently attached. The ML approaches the CQoSB to get QoS-related information about the MN's different networks. Upon receiving this information, the ML sets the INF bits and thus maps the Location_ID to the interface address.
- **Msg4**: A list of MN's Location_IDs along with their QoS specifications is passed to the CN, which chooses the route to the MN and thus defines the corresponding

Location_ID.

- **Msg5**: Since the CN has the MN's full address, the CN can start the connection by sending Access Request to the MN. This request will be intercepted by the AR in the source network which checks the Scope Field in the destination address. Based on the SF value, if MN was accessible for CN the access request packet is forwarded otherwise, it is dropped.
- **Msg6** When the access request gets to the destination network, the AR will check whether the request complies with the access policy or not. If the request passes the check, the AR passes it to the MN.

However, before the CN could use the service on MN, there is a need to achieve mutual authentication and set a secure session between the CN and the MN. This could be achieved using Authentication and Key Agreement (AKA) protocols similar to the one in [2]

3) Model Analysis and Attacks Modelling: This section will describe different attack scenarios and show how our security model react to them.

- The first scenario is the case of a Denial Of Service (DOS) Attack where a single Corresponding Node (CN) is trying to access a server with a LAN/Site scope. Obviously, if the CN was not in the server's scope, its connection request will be dropped by the Access Routers. Otherwise, it could communicate with the server. However, if the CN initially claims more QoS than it is allowed to, this will be detected by the Access Admission Enforcement (AAE) as violation to the access policy. Furthermore, after making the connection, if the CN tries to abuse the network and exceeds the reserved QoS, this will be detected by the Network Monitoring Entity (NME) module in the Access Router, consequently, the CN will be blacklisted.
- A similar discussion applies if the server was global.
- The third scenario considers the case of a Distributed Denial of Service (DDOS) attack where multiple corresponding nodes attempt to access a server with LAN or Site scope. Only corresponding nodes in the scope of the server could communicate with the server. However, in the case where a large number of legitimate nodes managed to access the server, they could overload the server and launch a DDOS attack despite the fact that none of the nodes has individually exceeded the agreed QoS.
- In case of a server with a global scope, the previous DDOS attack could still be achievable.

Furthermore, by deploying the new address scheme in Section VI-A, which uses the Node_ID to identify the device, if a multi-homed CN attempts to start multiple sessions with the server using different network interfaces, the network and thus the server will be able to co-locate these sessions to the same CN and thus monitor the resources utilization over the different sessions. Table IV summarizes the analysis result.

TABLE IV
ANALYSIS SUMMARY

Scope	DOS	DDOS
LAN/ Site	Fully Mitigated	Still Possible
Global	Fully Mitigated	Partially Mitigated

VII. CONCLUSION

This paper introduces a novel security model to limit servers accessibility over heterogeneous environments, which will help in mitigating some serious security threats such as denial of service attacks. This model adopts the QoSS concept to integrate security and QoS, it also benefits from recent enhancements on network services such as the enhanced DNS and Location servers to support the integration with the network infrastructure. The analysis section shows that, the proposed model succeeds in stopping DoS attacks while is partially effective in addressing Distributed DOS attacks.

REFERENCES

[1] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations". RFC 2663, August 1999.

[2] M. Aiash, G. Mapp, A. Lasebae, R. Phan, J. Loo,"A Formally Verified Initial AKA Protocol in Heterogeneous Environments Using Casper/FDR (Submitted For Publication)", International Journal of Information Security, Springer.

[3] H. Ballani, Y. Cathwathe, S. Ratnasamy, T. Roscoe and S. Shenker, "Off by Default".Proc.the 4th Workshop on Hot Topics in Networking (HotNets-II). 2005

[4] R. Bush and D. Meyer, "Some Internet Architectural Guidelines and Philosophy". RFC 3439, December 2002.

[5] C. Paquet, "Authorized Self-Study Guide Implementing Cisco IOS Network Security (IINS)" Indianapolis, USA: Cisco Press, 2009.

[6] P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION". RFC 1035, November 1987.

[7] G. Mapp, F. Shaikh, M. Aiash, R. P.Vanni, M. Augusto and E. Moreira, "Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Wireless Networks" ,Proc. International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS-09) August 2009.

[8] M. Aiash, G. Mapp, A. Lasebae, " A QoS Framework for Heterogeneous Networking", Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2011, WCE 2011, 6-8 July, 2011, London, U.K., pp1765-1769.

[9] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6",Internet Draft, 1997.

[10] R. Stewart, "Stream Control Transmission Protocol", RFC 4960, 2007.

[11] I. Ishiyama, K. Uehara, H. Esaki and F. Teraoka, "LINA: A New Approach to Mobility in Wide Area Networks", Proc. IEICE Trans. Commun., August 2001.

[12] M. Kunishi, M. Ishiyama, K. Uehara, H. Esaki and F. Teraoka, "LIN6: A New Approach to Mobility Support in IPv6", Proc. the International Symposium on Wireless Personal Multimedia Communication, 2006.

[13] G. Mapp, M. Aiash, H. C.Guardia and J. Crowcroft, "Exploring Multihoming Issues in Heterogeneous Environments",Proc. 1st International Workshop on Protocols and Applications with Multi-Homing Support (PAMS'11). Singapore.2011.

[14] M. Aiash, G. Mapp, A. Lasebae and R. Phan, M. Augusto, R. Vanni, E. Moreira, "Enhancing Naming and Location Services to support Multi-homed Devices in Heterogeneous Environments", Proc. The CCSIE 2011, London-UK, 25-27 July 2011.

[15] S. Jochen, "Mobile Communications". Addison Wesley, 2003

[16] M. Almeida, D. Corujo, S. Sargento, V. Jesus, and R. Aguiar, "An End-to-End QoS Framework for 4G Mobile Heterogeneous Environments", OpenNet Workshop (2007).

[17] P. Chandra, "Bulletproof wireless security : GSM, UMTS, 802.11 and ad hoc security". Newnes. Oxford, pp. 129-158, 2005.

[18] D. Durham, Ed, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol". RFC 2748. 2000.

[19] J.H. Schiller, "Mobile communications", 2nd ed. London, England: Addison-Wesley, 2003.

[20] Y-Comm Research. http://www.mdx.ac.uk/research/areas/\software/ycomm_research.aspx. [Accessed 19 August 2011].

[21] International Telecommunication Union (ITU), "Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services", ITU-T Recommendation Y.140.1, 2004.

[22] Institute of Electrical and Electronics Engineers. IEEE 802.21/D8.0, ”Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services”,2007.
[23] Long Term Evolution Protocol Overview, Freescale Semiconductor,2008. http://www.freescale.com/files/wireless_comm/doc/white_paper/LTEPTCLOVWWP.pdf. [Accessed 19 August 2011].
[24] D. Burgess and H. Samra, ”The Open BTS Project”,August 3, 2008. http://www.ahzf.de/itstuff/papers/OpenBTSProject.pdf
[25] T. E. Levin., C. E. Irvine., and E. Spyropoulou, ”Quality of Security Service: Adaptive Security”, The Handbook of Information Security, John Wiley and Sons. December 2005.
[26] E. Spyropoulou., T. E. Levin., C. E. Irvine., ”Calculating costs for quality of security service”, Proceedings of the 16th Computer Security Applications Conference, New Orleans, LA, December 2000, pp. 334-343
[27] T. E. Levin., C. E. Irvine., ”Quality of Security Service”, Proceedings of the New Security Paradigms Workshop, Ballycotton, Ireland, 18-22, September 2000.

Mahdi Aiash This author received his BEng degree in Computer Engineering from Aleppo University, Syria in 2004 and a Master Degree (MSc COMPUTER AND NETWORK SECURITY) from Middlesex University, London, UK in 2008. Currently, he is working towards a PhD in Security For future Heterogeneous Networks at Middlesex University.

He is a member of the Y-Comm research group and has participated in many conferences such as AICT’10 and ICWN’11 as a reviewer and session chair. In addition to a number of publications in reputable conferences and journals such as SECRYPT 2010, IEEE and Springer, he has a dozen of technical qualifications mainly related to Networking and Information Security.

Mr. Aiash is an Associate member of the IEEE and IEEE ComSoc since 2008. His paper titled ”A QoS Framework for Heterogeneous Networking” has been selected for the Best Student Paper Award of The 2011 International Conference of Wireless Networks in London.

Glenford Mapp This author received his PhD from the Computer Laboratory, University of Cambridge in 1992.

He is also a Principal Lecturer in Computer Networks at Middlesex University in North London and a Visiting Fellow in the LCE Technology Group at the Computer Laboratory, University of Cambridge. He worked on a number of networking-oriented projects and proposed the X-Windows Teleporting project, which later evolved into Virtual Network Computing, http://www.realvnc.com. He also led the early stages of the CLAN project, which developed very low latency networking technology for the local area. A new company in Cambridge called Level 5 Networks http://www.level5networks.com is bringing some exciting new low latency networking products to the marketplace. He is the chief architect of Y-Comm, a new architecture for future mobile communications systems. See:http://www.mdx.ac.uk/research/areas/software/ycomm_research.aspx. He is working, along with his colleagues at Middlesex, on developing performance models for mobile and distributed architectures. Currently he is working on proactive vertical handover algorithms, network memory storage systems, flexible transport protocols and network resilience.

Dr. Mapp is a Cambridge Commonwealth Fellow and a member of British Computer Society.

Aboubaker Lasebae This author got his BASc from the University Regina, Canada and his MSc from the University of Southampton, England and PhD from Middlesex University.

Currently, he is a principal lecturer at the School of Engineering and Information Systems and the director of postgraduate programmes for Computer Communications and the programme Leader of Computer and Network Security. He has several publications in the areas of QoS, Network Security, Wireless Networks and Mobile IP.

Dr. Lasebae is a member of the Institute of Electrical and Electronic Engineering (MIEEE) since 1985, and of The British Computer society (BCS) since 2009.